WHAT IS CLAIMED IS:

1. A method for detecting clones (unauthorized duplicate identities) of the client, the method comprising:

forwarding a first signal from a client to a KDC, the first signal for requesting access to a server;

verifying that the client is authorized to access the server;

transmitting a ticket from the KDC to the client, the ticket for providing access to the server, wherein the ticket is valid for a time T;

receiving a second signal from an entity, the second signal for requesting access to the server, wherein the entity has identifying information identical to the client; and

if the second request is received prior to expiration of the time T, either marking the entity as a possible clone or denying the second request in order to prevent access to the server.

2. The method of claim 1 further comprising

providing a session key in the ticket, the session key being valid for a designated duration.

3. The method of claim 2 wherein the designated duration is for determining the time T for which the ticket is valid.

4. A system for detecting clones of a client within a communication network, the system comprising:

a KDC;

an application server communicably coupled to the KDC;

a client for providing a first request to access the application server;

responsive to the first request, the KDC forwarding a first ticket for accessing the application server, the first ticket being valid for a time duration T;

the KDC receiving a second request to access the application server, the second request being received from an entity having identifying information identical to the client; and

if the second request is received during time T, the KDC denying the second request to prevent the entity from accessing the application server.

5. The system of claim 4 wherein the entity is a clone.

6. The system of claim 5 wherein the identifying information is a client identifier copied by the clone.

7. The system of claim 4 wherein the ticket further comprises an encrypted session key.

8. The system of claim 7 further comprising

the client deriving a copy of the session key for accessing the application server.

9. The system of claim 8 wherein the session key is derived using a key agreement algorithm.

10. The system of claim 9 wherein the key agreement algorithm is the Diffie-Hellman algorithm.

11. The method of claim 1 further comprising

using a key algorithm for authenticating communication between the KDC and the client such that all clients wishing access to the server are required to contact the KDC.

12. The method of claim 4 further comprising

requiring all entities wishing to access the server to communicate with the KDC.

13. A system for detecting clones (duplicate identities) of an authorized computing device in a communication network, the system comprising:

a first computing device;

a second computing device authorized to access the first computing device;

a key management means for providing to the second computing device, a session key for accessing the first computing device, the session key being invalid after a period T;

the key management means receiving one or more requests from an entity, to access the first computing device, the entity having identifying information identical to the second computing device; and

the key management means permitting the entity to access the first computing device, provided the number of access requests received during period T, is M or less requests.

14. The system of claim 13 wherein the key management means utilizes Diffie-Hellman key agreement algorithm to distribute session keys.

15. The system of claim 13 further comprising

the key management means flagging the entity if more than M requests are received from the entity.

16. The system of claim 13 wherein the identifying information is an identifier for the second computing device.

17. The system of claim 13 further comprising

the key management means denying access to the first computing device, if more than M requests are received.

18. A system for detecting clones of a client within a communication network, the system comprising:

a KDC;

a server communicably coupled to the KDC;

a client for receiving a ticket from the KDC, wherein the ticket is for accessing the server, and is valid for a time duration T;

the server receiving from the client a first request to access the server, the first request being accompanied by the ticket;

the server recording the time duration T for which ticket is valid;

the server receiving from an entity, a second request to access the server, the entity having identifying information identical to the client and

the server either flagging or denying the second request to prevent access to the server, if the second request is received during the time duration T.

19. The system of claim 18 further comprising

the KDC encrypting a session key within the ticket; and

the client extracting a copy of the session key in a manner that no entity other than the client can access the session key.

20. The system of claim 18 further comprising

necessitating by the system, all clients wishing to access the server to communicate with the KDC.

21. The method of claim 18 wherein a ticket granting server is the server, and the ticket is a ticket granting ticket.

22. A method for detecting clones in a communication network, the method comprising:

providing a ticket to an authorized client, the ticket for accessing a KDC, the ticket having a session key valid for a time duration T;

receiving a request to access the KDC, the request being received from an entity with the same identifying information as the authorized client; and

if the request is received during time T, flagging the entity as a possible clone or denying the request to access to the KDC.

23. The method of claim 22 wherein the ticket is a TGT (ticket granting ticket).

24. The method of claim 1 wherein the KDC marks the entity as a possible clone or denies the second request in order to prevent access to the server.

25. The method of claim 1 wherein the server marks the entity as a possible clone or denies the second request in order to prevent access to the server.

26. The method of claim 18 wherein the KDC is the server.